What is claimed is:

1. A license management method for use in a license management system wherein license management of software installed on a user terminal is performed using a private key and a public key in a public key cryptosystem, said license management system comprising a product management server that issues an identification code identifying a software product; an authentication server that has a database recording therein license information including the identification code and a terminal code identifying a user terminal and that compares information sent from said user terminal with the license information; and a route server that creates a digital signature used as a basis of authentication, said license management method comprising:

a first digital signature creation step of creating, by said product management server, a first digital signature from the identification code using a private key of said product management server, said first digital signature being attached to the software product;

a second digital signature creation step, by said route server, of obtaining a public key of said product management server from said product management server and creating a second digital signature from the public key of said product management server using a private key of said route server;

a third digital signature creation step, by said route server, of obtaining a public key of said authentication server from said authentication server and creating a third digital signature from the public key of said authentication server using the private key of said route server;

a first checking step, by said authentication server, of checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public

key of said product management server;

a second checking step, by said authentication server, of checking validity of the first digital signature using the public key of said product management server in response to the first digital signature and the terminal code from said user terminal and, based on the checking result, obtaining the identification code;

a recording step, by said authentication server, of comparing the identification code and the terminal code with the license information recorded in the database and, if a predetermined condition is satisfied, recording the identification code and the terminal code in the database;

a fourth digital signature creation step, by said authentication server, of creating a fourth digital signature from the identification code and the terminal code using a private key of said authentication server;

a third checking step, by said user terminal, of checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said authentication server;

a fourth checking step, by said user terminal, of checking validity of the fourth digital signature using the public key of said authentication server obtained in said third checking step and, based on the checking result, obtaining the identification code and the terminal code; and

a limitation release step, by said user terminal, of releasing a functional limitation of the software based on the checking result of said fourth checking step.

2. The license management method according to claim 1,

wherein said authentication server has a server expiration date indicating an expiration date of the third digital signature,

wherein, in said third digital signature creation step, said route server obtains the public key of said authentication server and the server expiration date from said authentication server and, using the private key of said route server, creates a digital signature of said authentication server from the public key of said authentication server and the server expiration date, and

wherein, in said third checking step, said user terminal checks validity of the digital signature of said authentication server using the public key of said route server obtained from said route server and obtains the server expiration date and the public key of said authentication server,

further comprising a comparison step of comparing the server expiration date with a current date, said server expiration date being verified as valid in said third checking step.

3. The license management method according to claim 1

wherein said authentication server has a software expiration date indicating an expiration date of the software,

wherein, in said fourth digital signature creation step, a digital signature of said terminal is created from the identification code, the terminal code, and the software expiration date using the private key of said authentication server,

wherein, in said fourth checking step, said user terminal checks validity of the fourth digital signature using the public key of said authentication server obtained from said authentication server and obtains the identification code, the terminal code, and the software expiration date, and

wherein, in said limitation release step, the functional limitation of the installed software is released based on the software expiration date verified as valid in said fourth checking step.

4. A license management system comprising a user terminal on which a software product is installed; a product management server that issues an identification code identifying the software product; an authentication server that has a database recording therein license information including the identification code and a terminal code identifying said user terminal and that compares information sent from said user terminal with the license information; and a route server that creates a digital signature used as a basis of authentication,

wherein said product management server comprises:

first digital signature creation means for creating a first digital signature from the identification code using a private key of said product management server, said first digital signature being attached to the software product,

wherein said route server comprises:

second digital signature creation means for obtaining a public key of said product management server from said product management server and for creating a second digital signature from the public key of said product management server using a private key of said route server; and

third digital signature creation means for obtaining a public key of said authentication server from said authentication server and for creating a third digital signature from the public key of said authentication server using the private key of said route server;

wherein said authentication server comprises:

first checking means for checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, for obtaining the public key of said product management server;

second checking means for checking validity of the first digital signature using the public key of said product management server in response to the first digital signature and the terminal code from said user terminal and, based on the checking result, for obtaining the identification code;

recording means for comparing the identification code and the terminal code with the license information recorded in the database and, if a predetermined condition is satisfied, for recording the identification code and the terminal code in the database; and

fourth digital signature creation means for creating a fourth digital signature from the identification code and the terminal code using a private key of said authentication server; and

wherein said user terminal comprises:

third checking means for checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, for obtaining the public key of said authentication server;

fourth checking means for checking validity of the fourth digital signature using the public key of said authentication server obtained from said third checking means and, based on the checking result, for obtaining the identification code and the terminal code; and

limitation release means for releasing a functional limitation of the software based on the checking result of said fourth checking means.

5. The license management system according to claim 4,

wherein said authentication server has a server expiration date indicating an expiration date of the third digital signature,

wherein said third digital signature creation means in

said route server obtains the public key of said authentication server and the server expiration date from said authentication server and, using the private key of said route server, creates a digital signature of said authentication server from the public key of said authentication server and the server expiration date,

wherein said third checking means checks validity of the digital signature of said authentication server using the public key of said route server obtained from said route server and obtains the server expiration date and the public key of said authentication server, and

wherein said user terminal further comprises comparison means for comparing the server expiration date with a current date, said server expiration date being verified as valid by said third checking means.

6. The license management system according to claim 4

wherein said authentication server has a software expiration date indicating an expiration date of the software,

wherein said fourth digital signature creation means creates a digital signature of said terminal from the identification code, the terminal code, and the software expiration date using the private key of said authentication server,

wherein said fourth checking means checks validity of the fourth digital signature using the public key of said authentication server obtained from said authentication server and obtains the identification code, the terminal code, and the software expiration date, and

wherein said limitation release means releases the functional limitation of the installed software based on the software expiration date verified as valid by said fourth checking means.